

## CLAIMS

1. A method of performing point doublings comprising:  
generating a first point doubling using an initial point (x, y) comprising generating  
5 a current slope value and a current x value;  
generating a second point doubling comprising generating a new current x value  
and new current slope value without using a multiplication step.
2. The method of claim 1 wherein said generating said second point doubling  
10 comprises generating a new current x value and new current slope value without using a y  
term.
3. The method of claim 1 wherein said generating said second point doubling  
comprises storing said current x value as a prior x value and storing said current slope  
15 value as a prior slope value; generating a new current x value using said prior slope value;  
and generating a new current slope value using said new current x value and said prior x  
value.
4. The method of claim 3 wherein said new current x value is generated by:  
20  $x_I = s^2 + s + a$   
where s is said prior slope value.

5. The method of claim 3 wherein said new current slope value is generated

by:

$$g = (x + x_1)^2 / x_1 + (s+1)$$

where x is said prior x value and x1 is said current x value.

5